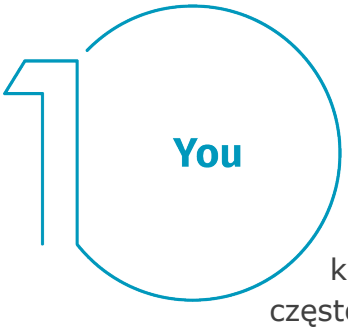
5 zasad bezpiecznej pracy z domu

Zdajemy sobie sprawę, że praca zdalna to dla niektórych osób nowość i przystosowanie się do nowych warunków może być trudne. Do naszych celów należy umożliwienie ci jak najbezpieczniejszej pracy w domu. Poniżej znajduje się pięć prostych kroków zapewniających bezpieczeństwo. Co najważniejsze, wszystkie te działania nie tylko chronią twoją pracę, ale także ciebie i twoją rodzinę podczas dbania o bezpieczeństwo domowej cyberprzestrzeni.



Ty: Przede wszystkim sama technologia cię nie ochroni – to ty stanowisz najlepszą obronę. Przestępcy zrozumieli, że najłatwiej osiągnąć to, czego chcą, biorąc na cel bezpośrednio ciebie, a nie twój komputer lub inne urządzenia. Jeśli chcą przejąć twoje hasło, dane firmowe lub kontrolę nad twoim komputerem, spróbują cię oszukać, często stwarzając wrażenie pilności. Na przykład mogą zadzwonić, podając się za pomoc techniczną firmy Microsoft, i poinformować, że twój komputer został zainfekowany. Mogą też wysłać e-mail z ostrzeżeniem, że nie udało się dostarczyć paczki, nakłaniając cię do kliknięcia w złośliwy odnośnik. Częste oznaki ataku socjotechnicznego to:

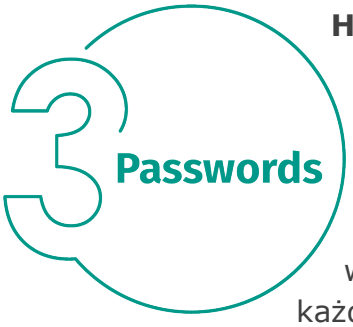
- Wywoływanie uczucia, że sprawa jest niezwykle pilna, poprzez zastraszanie, informację o kryzysie lub ważnym zleceniu. Cyberprzestępcy potrafią tworzyć przekonujące wiadomości, podszywając się w nich pod zaufane instytucje, takie jak banki, rząd lub organizacje międzynarodowe.
- Nacisk, aby ominąć bądź zignorować zasady lub procedury bezpieczeństwa, albo oferta zbyt piękna, by była prawdziwa (nie, nie masz wygranej na loterii!).
- Wiadomość od współpracownika lub znajomego, ale podpis, ton lub treść nie pasują do tej osoby.

Najlepszą obroną przed atakami tego rodzaju jesteś ty.

Sieć domowa: Prawie każda sieć domowa zaczyna się od sieci bezprzewodowej (często nazywanej Wi-Fi). To dzięki niej twoje urządzenia mogą łączyć się z Internetem. Większość domowych sieci bezprzewodowych jest kontrolowana przez router internetowy albo oddzielny, dedykowany bezprzewodowy punkt dostępu. Oba działają tak samo: emitują sygnały bezprzewodowe, z którymi łączą się urządzenia domowe. Oznacza to, że zabezpieczenie sieci Wi-Fi to kluczowy element ochrony domu. Zalecamy podjęcie następujących kroków, by ją zabezpieczyć:

- Zmień domyślne hasło administratora urządzenia kontrolującego twoją sieć bezprzewodową. Konto administratora umożliwia skonfigurowanie ustawień sieci Wi-Fi.
- Zapewnij, że tylko zaufane osoby będą mogły łączyć się z twoją siecią bezprzewodową. Zrób to, włączając silną ochronę. Gdy opcja zostanie włączona, połączenie z twoją siecią Wi-Fi będzie wymagało podania hasła. Po połączeniu działania użytkowników sieci będą szyfrowane.
- Upewnij się, że hasło używane do łączenia się z siecią bezprzewodową jest silne i różni się od hasła administratora. Pamiętaj, że hasło należy podać tylko raz dla każdego z urządzeń, ponieważ jest ono przez nie zapamiętywane i przechowywane.

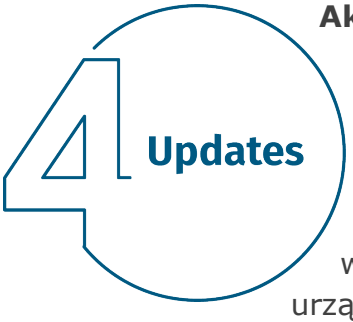
Nie wiesz, jak wykonać te kroki? Zwróć się do dostawcy Internetu, zajrzyj na jego stronę internetową, zapoznaj się z instrukcją obsługi bezprzewodowego punktu dostępowego albo wejdź na stronę sprzedawcy.



Hasła: Kiedy strona poprosi cię o stworzenie hasła – utwórz silne hasło, im więcej znaków zawiera, tym jest ono silniejsze. Jednym z najprostszych sposobów na silne hasło jest zastosowanie wyrażenia hasłowego. Wyrażenie hasłowe to po prostu hasło składające się z kilku słów, np. *„bourbon z miodem pszczelim”*. Użycie unikalnego wyrażenia hasłowego oznacza przypisanie innego do każdego urządzenia lub konta w sieci. Dzięki temu, jeśli jedno z wyrażeń hasłowych zostanie przejęte, twoje pozostałe konta i urządzenia nadal będą bezpieczne. Nie pamiętasz wszystkich swoich wyrażeń hasłowych?

Użyj menedżera haseł – jest to specjalny program, który bezpiecznie przechowuje wszystkie wyrażenia hasłowe w zaszyfrowanej postaci (ma też wiele innych świetnych funkcji!). I wreszcie – włącz weryfikację dwuetapową,

zwaną także uwierzytelnianiem dwuskładnikowym, gdy jest to możliwe. Korzysta ona z twojego hasła, ale także dodaje drugi krok, np. kod wysyłany na smartfona lub generowany przez aplikację. Weryfikacja dwuetapowa to zapewne najważniejsze działanie, jakie można przedsięwziąć w celu ochrony kont w sieci. Jest ona łatwiejsza, niż ci się wydaje.



Aktualizacje: Upewnij się, że używasz najnowszej wersji oprogramowania na wszystkich komputerach i urządzeniach przenośnych, a programy i aplikacje są zaktualizowane. Cyberprzestępcy wciąż szukają nowych luk w oprogramowaniu twoich urządzeń. Gdy odkryją słabe punkty, posługują się specjalnymi programami, by je wykorzystać, i włamują się do systemów operacyjnych urządzeń, których używasz. Tymczasem firmy, które stworzyły oprogramowanie tych urządzeń, ciężko pracują nad aktualizacjami likwidującymi luki w zabezpieczeniach. Zapewniając, że te aktualizacje będą niezwłocznie instalowane na twoich komputerach i urządzeniach przenośnych, poważnie utrudnisz dokonanie włamania. Aby pozostać na bieżąco, po prostu włącz automatyczne aktualizacje, kiedy to tylko możliwe. Ta zasada dotyczy niemal każdego produktu połączonego z siecią, w tym nie tylko urządzeń firmowych, ale także telewizorów mogących łączyć się z Internetem, elektronicznych niań, kamer monitoringu, routerów domowych, konsol do gier, a nawet twojego samochodu.

Dzieci/goście: W biurze najprawdopodobniej nie musisz martwić się gośćmi, dziećmi albo innymi członkami rodziny korzystającymi z twojego służbowego laptopa lub innych urządzeń. Upewnij się, że rodzina i znajomi rozumieją, że nie wolno im używać sprzętu, na którym pracujesz, ponieważ mogą przypadkowo usunąć lub zmodyfikować dane albo co gorsza – zainfekować urządzenie.